IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

KAITLYN THIEL, ***individually and on behalf of all others similarly situated,***	**Case No. _____**
Plaintiff,	**Judge _____**
v.	**Magistrate Judge _____**
Marshall & Melhorn, LLC,	**CLASS ACTION COMPLAINT**
Defendant.	**JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Kaitlyn Thiel ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant Marshall & Melhorn, LLC ("Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Defendant, a law firm in Northwest Ohio.

2. Defendant failed to properly safeguard the personally identifiable information ("PII") that it collected and maintained as part of its regular business activities including Social Security Numbers and full names.

3. As a result of Defendant's failures, Plaintiff and over 27,000 other individuals ("Class Members") have had their most sensitive personal information stolen and publicly

published on the internet. The information that was published to the internet allows for one-stop shopping for identity thieves to wreak complete havoc on their victims' lives.

4. Moreover, given the sensitivity and static nature of the information involved (including Social Security numbers), Plaintiff and Class Members will be forced to live with the present and continuing threat of a data breach for the remainder of their lives.

5. Defendant collected and maintained certain personally identifiable information of Plaintiff and the putative class (defined below), who are (or were) employees at Defendant..

6. Businesses that collect and store their current and former employees' PII have statutory, regulatory, contractual, and common law duties to safeguard that information and ensure it remains private.

7. Plaintiff and those similarly situated relied upon Defendant to maintain the security and privacy of the PII entrusted to it. Plaintiff and Class Members reasonably expected and understood that Defendant would comply with its obligations to keep the PII secure and safe from unauthorized access and to delete PII that was not reasonably necessary to hold for a legitimate business purpose.

8. Defendant is responsible for allowing this data breach through its failure to implement and maintain reasonable network safeguards, its unreasonable data retention policies, its failure to adequately train employees, and its failure to comply with industry-standard data security practices.

9. Plaintiff and members of the proposed Class have suffered actual and imminent injuries as a direct result of the data breach. The actual and imminent injuries suffered by Plaintiff and the proposed Class as a direct result of the Data Breach include: (i) Plaintiff experiencing fraudulent charges to her Chase account in February 2023; (ii) Plaintiff experiencing identity theft

in the form of a Chase credit card being opened under her name; (iii) Plaintiff experiencing identity theft in the form of an investment account being fraudulently opened at Ally Bank under her name; (iv) Plaintiff experiencing identity theft in the form of an identity thief accessing her account at Huntington relating to a car loan; (v) Plaintiff's PII being disseminated on the Dark Web, according to Norton; (vi) Plaintiff's out-of-pocket costs for credit monitoring and identity theft insurance; (vii) an increase in spam calls, texts, and/or emails; (viii) invasion of privacy; (ix) loss of benefit of the bargain; (x) lost time spent on activities remedying harms resulting from the Data Breach; (xi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (xii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect her Private Information.

10. Accordingly, Plaintiff, on behalf of herself and other members of the Class (as defined infra), asserts claims for negligence, negligence *per* se, breach of implied contract, and unjust enrichment, and seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

PARTIES

Plaintiff Kaitlyn Thiel

11. Plaintiff Kaitlyn Thiel is a natural person and resident and citizen of Edon, Ohio.

Defendant Marshall & Melhorn, LLC

12. Defendant is a domestic limited liability company formed in Ohio and headquartered in Toledo, Ohio. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

13. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant, establishing sufficient minimal diversity.[1]

14. The Northern District of Ohio has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Ohio and this District through its headquarters, offices, parents, and affiliates.

15. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Business

16. Defendant is a law firm in Northwest Ohio with offices in Toledo, Findlay, and Perrysburg.[2]

17. Upon information and belief, in the course of collecting PII from employees, including Plaintiff, Defendant promised to provide confidentiality and adequate security for employee data through its applicable privacy policy and through other disclosures in compliance

[1] According to the report submitted to the Office of the Maine Attorney General, 8 Maine residents were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/e3cf578c-bdbe-4218-b518-ec1d57d461b7.shtml (last visited June 15, 2023).

[2] https://www.marshall-melhorn.com/Offices (last visited: June 16, 2023).

with statutory privacy requirements.

18. Indeed, Defendant's Privacy Policy provides that: "[i]nformation provided to Marshall Melhorn is treated with care and discretion. . . we strive to ensure the information is kept private and not misused[.]"[3]

19. Plaintiff and the Class Members, as former and current employees of Defendant, relied on these promises and on this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Employees, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

20. In the course of their employment relationship, employees, including Plaintiff and Class Members, provided Defendant with at least the following PII: names and Social Security numbers.

21. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

22. On September 14, 2021, Defendant experienced a computer outage on its network.[4]

23. On or about June 7, 2023, Defendant sent Notice of Security Incident letters (the "Notice Letter") to approximately 27,271 individuals whose PII was compromised in the Data Breach, informing those individuals that "files within our network may have been accessed and

[3] https://www.marshall-melhorn.com/Privacy-Policy (last visited: June 16, 2023).
[4] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/e3cf578c-bdbe-4218-b518-ec1d57d461b7.shtml (last visited June 15, 2023).

acquired by the unauthorized actor but [we were] unable to determine precisely all files which were subject to this unauthorized activity," and that, after review, Defendant learned that Plaintiff's and Class Member's PII was within the compromised files.[5]

24. The PII compromised in the Data Breach included individuals' names and Social Security numbers.

25. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the PII of Plaintiff and Class Members.

26. As evidenced by the Data Breach's occurrence, the PII contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

27. Plaintiff's PII was accessed and stolen in the Data Breach and Plaintiff believes her stolen PII is currently available for sale on the dark web because that is the *modus operandi* of cybercriminals.

28. Due to the actual and imminent risk of identity theft as a result of the Data Breach, Plaintiff and Class Members must, as Defendant's Notice Letter instructs them, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.[6]

29. In the Notice Letter, Defendant makes an offer to provide identity monitoring services for a period of no longer than 24 months. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized

[5] *Id.*
[6] *Id.*

release and disclosure of Plaintiff's and Class Members' PII.

30. That Defendant is encouraging its current and former employees to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted individuals' PII *was* accessed, thereby subjecting Plaintiff and Class Members to a substantial and imminent threat of fraud and identity theft.

31. Defendant had obligations created by contract, state and federal law, common law, and industry standards to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

Securing PII and Preventing Breaches

32. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members, by properly training its employees to recognize and prevent cybersecurity risks, and/or by destroying the data it no longer needed.

33. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

34. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[7]

[7] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

35. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[8]

36. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
>
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
>
> - Prioritize and treat commodity malware infections as potential full compromise;
>
> **Include IT Pros in security discussions**
>
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> **Build credential hygiene**
>
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
>
> **Apply principle of least-privilege**
>
> - Monitor for adversarial activities
> - Hunt for brute force attempts
> - Monitor for cleanup of Event Logs
> - Analyze logon events;
>
> **Harden infrastructure**

[8] *Id.* at 3-4.

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[9]

37. Given that Defendant was storing the sensitive PII of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

38. And, even absent the warnings by the FBI and others, Defendant was aware of the need to protect sensitive data collected by businesses and published a memorandum advising business of the need to "take[] reasonable cybersecurity precautions conforming to "industry recognized framework."[10]

39. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of over 27,000 individuals, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores Employees' PII

40. Defendant acquires, collects, and stores a massive amount of PII on its employees, former employees and other personnel.

41. As a condition of employment or as a condition of receiving certain benefits, Defendant requires that employees, former employees and other personnel entrust it with highly sensitive personal information.

---

[9] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

[10] https://www.marshall-melhorn.com/portalresource/lookup/wosid/cp-base-4-4607/media.name=/33F8730-August%202018%20Client%20Memo.PDF

42. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

43. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

44. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew or Should Have Known of the Risk Because Employers In Possession Of PII Are Particularly Suspectable To Cyber Attacks

45. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII, like Defendant, preceding the date of the breach.

46. Data breaches, including those perpetrated against employers that store PII in their systems, have become widespread.

47. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[11]

48. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[12]

49. In light of recent high profile data breaches at industry leading companies,

[11] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[12] *Id*.

including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

50. Defendant knew and understood unprotected or exposed PII in the custody of employers, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

51. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

52. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

53. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

54. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

55. As a law firm in custody of current and former employees' PII, Defendant knew,

or should have known, the importance of safeguarding PII entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

The Value of PII

56. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[14]

57. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[15]

58. For example, Personal Information can be sold at a price ranging from $40 to $200.[16]

[13] 17 C.F.R. § 248.201 (2013).
[14] *Id.*
[15] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).
[16] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).

59. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[17]

60. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems. [18]

61. It is incredibly difficult to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

62. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19]

---

[17] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).
[18] Identity Theft and Your Social Security Number, Social Security Administration, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 13, 2021).
[19] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR

63. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, only credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach, including Social Security number and name, is impossible to "close" and difficult, if not impossible, to change.

64. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[20]

65. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

66. The fraudulent activity resulting from the Data Breach may not come to light for years.

67. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

(Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-hasmillionsworrying-about-identity-theft (last accessed Jan. 17, 2022).

[20] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 17, 2022).

[21] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last accessed Jan. 17, 2022).

68. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

Defendant Fails To Comply With FTC Guidelines

69. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

70. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[22]

71. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[23]

72. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex

[22] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).
[23] *Id.*

passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

73. The FTC has brought enforcement actions against employers for failing to protect employee data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

74. These FTC enforcement actions include actions against employers over the compromised PII of its employees, like Defendant here.

75. Defendant failed to properly implement basic data security practices.

76. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

77. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails To Comply With Industry Standards

78. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

79. Several best practices have been identified that a minimum should be

implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

80. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

81. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

82. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES & DAMAGES

83. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; I invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

The Data Breach Increases Victims' Risk Of Identity Theft

84. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

85. The unencrypted PII of Class Members will end up for sale on the dark web, and in fact, it has already been published on the Dark Web. In addition, unencrypted PII may now fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

86. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

87. Because a person's identity is akin to a puzzle with multiple data points, the more

accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

88. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

89. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[24]

90. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

[24] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

91. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

92. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

93. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

94. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

95. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

96. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as signing up for credit monitoring and identity theft

insurance, contacting credit bureaus to place freezes on their accounts, securing their online accounts, contacting banks to secure their financial accounts, contacting third parties to resolve the fraud and identity theft that they experienced, and closing accounts that were compromised by identity thieves.

97. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[25]

98. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[26]

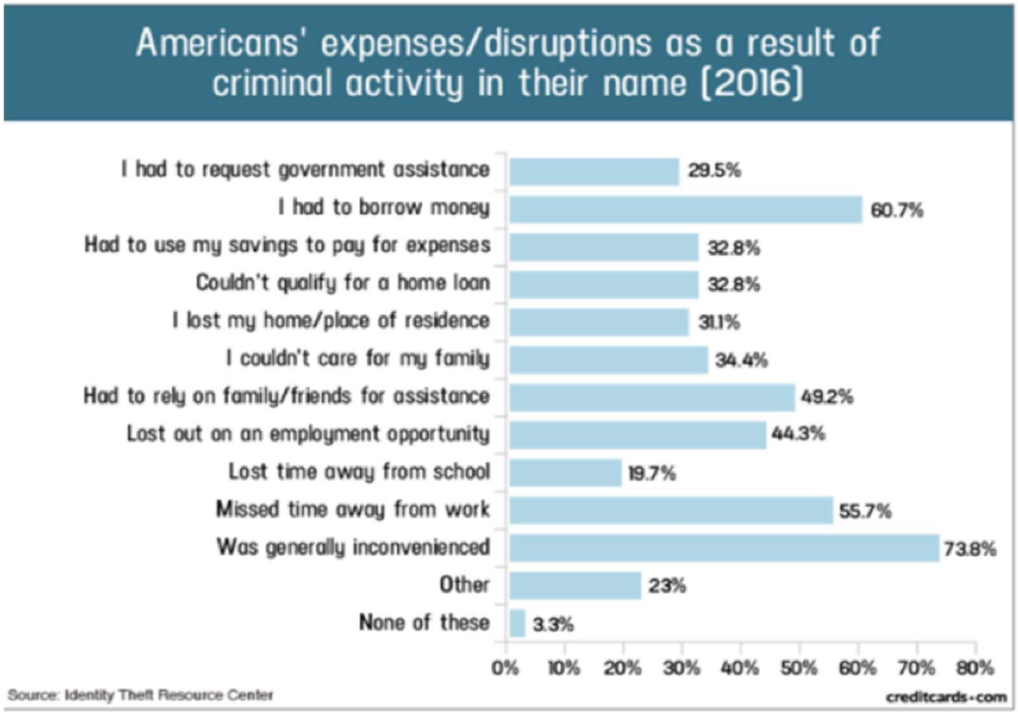
99. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[27]

---

[25] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[26] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

[27] Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Sep 13, 2022).



100. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

Diminution Value Of PII

101. PII is a valuable property right.[29] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

---

[28] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

[29] *See, e.g.,* Kaitlyn T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

102. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[30]

103. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[31,32]

104. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[33]

105. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

106. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., Social Security numbers and names.

107. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

---

[30] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[31] https://datacoup.com/
[32] https://digi.me/what-is-digime/
[33] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

108. The fraudulent activity resulting from the Data Breach may not come to light for years.

109. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

110. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially over 27,000 thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

111. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

112. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, the volume of data obtained in the Data Breach, and the reports of Plaintiff's PII already being disseminated on the dark web (as discussed below), there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

113. Such fraud may go undetected until debt collection calls commence months, or

even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

114. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[34] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

115. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

116. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Loss Of The Benefit Of The Bargain

117. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When submitting PII to Defendant under certain terms through a job application and/or onboarding paperwork, Plaintiff and other reasonable employees understood and expected that Defendant would properly safeguard and protect their PII, when in

[34] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received an employment position of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFF THIEL'S EXPERIENCE

118. Prior to the Data Breach, Plaintiff Thiel was employed at Defendant from approximately 2017 to 2018.

119. In the course of enrolling in employment with Defendant and as a condition of employment, she was required to supply Defendant with her PII–– including, but not limited to, her name and Social Security number.

120. Plaintiff Thiel received a Notice of Security Incident letter from Defendant, dated June 7, 2023, stating that it had determined an unauthorized actor gained access to files on its system, containing Plaintiff's name and Social Security number.

121. The letter stated, in relevant part, as follows:

> **What Happened?**
>
> On September 14, 2021, [Defendant] experienced an outage to [its] computer network. [Defendant] immediately launched an investigation with the help of computer specialists to determine the nature and scope of the incident and remediated the disruption. [Defendant's] investigation determined that the network outage was caused by an unauthorized actor who gained access to the Marshall Melhorn network. Unfortunately, this investigation determined that files within [its] network may have been accessed and acquired by the unauthorized actor but was unable to determine precisely all files which were subject to this unauthorized activity.
>
> In an abundance of caution, an analysis was undertaken on all potentially impacted files to determine what information may have been involved who that information related to, and contact information for such individuals. This review was completed on March 6, 2023. This review found that information regarding you may have been included in those files.
>
> **What Information was Involved?** The investigation determined that your Social Security number and name may have been accessed and/or acquired by an unauthorized actor.

122. Upon receiving the Notice Letter from Defendant, Plaintiff Thiel has spent significant time dealing with the consequences of the Data Breach including signing up for credit monitoring and identity theft insurance, contacting credit bureaus to place freezes on her accounts, securing her online accounts, contacting banks to secure her financial accounts, contacting third parties to resolve the fraud and identity theft that she experienced, and closing accounts that were compromised by identity thieves.

123. Plaintiff Thiel is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

124. At the time of the Data Breach—on or about September 14, 2021—Defendant retained Plaintiff's PII in its system, despite no longer maintaining an employment relationship with Plaintiff for approximately five years.

125. Subsequent to the Data Breach, Plaintiff Thiel has suffered numerous, substantial injuries including, but not limited to: (i) fraudulent charges to her Chase account in February 2023; (ii) identity theft in the form of a Chase credit card being opened under her name; (iii) identity theft in the form of an investment account being fraudulently opened at Ally Bank under her name; (iv) identity theft in the form of an identity thieve accessing her account at Huntington, relating to a car loan; (v) her PII being disseminated on the Dark Web, according to Norton; (vi) out-of-pocket costs for credit monitoring and identity theft insurance; (vii) an increase in spam calls, texts, and/or emails; (viii) invasion of privacy; (ix) loss of benefit of the bargain; (x) lost time spent on activities remedying harms resulting from the Data Breach; (xi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (xii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and

available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect her Private Information.. Plaintiff has spent significant time remedying the breach—approximately 20 hours thus far–valuable time that Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

126. Plaintiff Thiel additionally suffered actual injury and damages as a result of the Data Breach. Implied in her employment contract with Defendant was the requirement that it adequately safeguard her PII and that it would delete or destroy her PII after Defendant was no longer required to retain it. Plaintiff Thiel would not have worked for Defendant had Defendant disclosed that it lacked data security practices adequate to safeguard PII.

127. Plaintiff Thiel further suffered actual injury in the form of damages and diminution in the value of her PII —a form of intangible property that she entrusted to Defendant for the purpose of employment, which was compromised by the Data Breach.

128. Plaintiff Thiel also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially her Social Security number, being in the hands of criminals.

129. Plaintiff Thiel has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII being placed in the hands of unauthorized third parties and possibly criminals.

130. Plaintiff Thiel has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant’s possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

131. Plaintiff brings this nationwide class action on behalf of herself and all others similarly situated under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

132. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> **All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a Notice of Security Incident letter (the "Class").**

133. Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

134. Plaintiff reserves the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

135. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of more than 27,000 current and former employees of Defendant's whose sensitive data was compromised in Data Breach.[35]

136. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or

[35] https://apps.web.maine.gov/online/aeviewer/ME/40/e3cf578c-bdbe-4218-b518-ec1d57d461b7.shtml (last visited June 15, 2023).

disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant breached a fiduciary duty to Plaintiff and Class Members;

n. Whether Defendant breach implied or express contracts with Plaintiff and Class Members;

o. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

p. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

q. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

137. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

138. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

139. Predominance. Defendant have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

140. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class

Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

141. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

142. Plaintiff re-alleges and incorporates each of the foregoing paragraphs as if fully set forth herein.

143. Defendant required Plaintiff and Class Members to submit non-public PII as a condition of employment or as a condition of receiving employee benefits.

144. Plaintiff and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information and delete it once the employment relationship terminated.

145. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft.

Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

146. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

147. Section 5 of the FTC Act, as interpreted and enforced by the FTC, prohibits the unfair act or practice by businesses, such as Defendant,[36] of failing to use reasonable measures to protect PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII.

148. Plaintiff and members of the Class are within the class of persons that the FTC Act was intended to protect.

149. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against employers, which, as a result of failures to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm to its employees as that suffered by Plaintiff and members of the Class.

150. Defendant's conduct constitutes negligence because it was in violation of Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with

[36] https://www.ftc.gov/news-events/news/press-releases/2011/05/ftc-settles-charges-against-two-companies-allegedly-failed-protect-sensitive-employee-data

applicable industry standards.

151. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Class due to the valuable nature of the PII at issue in this case—including Social Security numbers.

152. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

153. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII; and,

e. Failing to detect in a timely manner that Class Members' PII had been compromised.

154. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the

industry.

155. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

156. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class.

157. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: (i) Plaintiff experiencing fraudulent charges to her Chase account in February 2023; (ii) Plaintiff experiencing identity theft in the form of a Chase credit card being opened under her name; (iii) Plaintiff experiencing identity theft in the form of an investment account being fraudulently opened at Ally Bank under her name; (iv) Plaintiff experiencing identity theft in the form of an identity thieve accessing her account at Huntington, relating to a car loan; (v) Plaintiff's PII being disseminated on the Dark Web, according to Norton; (vi) Plaintiff's out-of-pocket costs for credit monitoring and identity theft insurance; (vii) an increase in spam calls, texts, and/or emails; (viii) invasion of privacy; (ix) loss of benefit of the bargain; (x) lost time spent on activities remedying harms resulting from the Data Breach; (xi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (xii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect her Private Information.

158. Plaintiff and Class Members are entitled to compensatory and consequential

damages suffered as a result of the Data Breach.

159. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to The Class.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

160. Plaintiff re-alleges and incorporates each of the foregoing paragraphs as if fully set forth herein.

161. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

162. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

163. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se.*

164. Class Members are consumers within the class of persons that Section 5 of the FTC Act was intended to protect.

165. Moreover, the harm that has occurred is the type of harm that the FTC Act intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against

businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

166. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

167. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

168. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) Plaintiff experiencing fraudulent charges to her Chase account in February 2023; (ii) Plaintiff experiencing identity theft in the form of a Chase credit card being opened under her name; (iii) Plaintiff experiencing identity theft in the form of an investment account being fraudulently opened at Ally Bank under her name; (iv) Plaintiff experiencing identity theft in the form of an identity thieve accessing her account at Huntington, relating to a car loan; (v) Plaintiff's PII being disseminated on the Dark Web, according to Norton; (vi) Plaintiff's out-of-pocket costs for credit monitoring and identity theft insurance; (vii) an increase in spam calls, texts, and/or emails; (viii) invasion of privacy; (ix) loss of benefit of the bargain; (x) lost time spent on activities remedying harms resulting from the Data Breach; (xi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (xii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third

parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect her Private Information.

169. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

170. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

171. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

172. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

173. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

174. Plaintiff re-alleges and incorporates each of the foregoing paragraphs as if fully

set forth herein.

175. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their employment with Defendant.

176. Plaintiff and Class Members provided their labor and their PII to Defendant in exchange for (among other things) Defendant's promise to protect their PII from unauthorized disclosure and to delete it once it was no longer necessary to maintain the PII for employment purposes. Defendant additionally promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

177. On information and belief, Defendant further promised to and represented it would comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

178. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

179. When Plaintiff and Class Members provided their PII to Defendant as a condition of their employment, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

180. Defendant required Class Members to provide their PII as a condition of

employment. Plaintiff and Class Members accepted Defendant's offers and provided their PII and agreed to employment at Defendant.

181. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

182. Plaintiff and Class Members would not have entrusted their PII to Defendant or accepted employment at Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

183. Plaintiff and Class Members would not have entrusted their PII to Defendant or accepted employment at Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

184. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

185. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

186. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

187. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

188. Plaintiff and Class Members are also entitled to nominal damages for the breach of implied contract.

189. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to The Class.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

190. Plaintiff re-alleges and incorporates each of the foregoing paragraphs as if fully set forth herein.

191. This count is pleaded in the alternative to the Breach of Implied Contract claim above (Count III).

192. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of their labor and by providing their valuable PII to Defendant.

193. Plaintiff and Class Members provided Defendant their labor and PII on the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures from the revenue it derived therefrom. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

194. Defendant benefited from receiving Plaintiff's and Class Members' labor and from receiving their PII through its ability to retain and use that information for its own benefit. Defendant understood and accepted this benefit.

195. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

196. Because all PII provided by Plaintiff and Class Members was similarly at risk from a foreseeable and targeted data breach, Defendant's obligation to safeguard the PII it collected was

inherent to the relationship.

197. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

198. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

199. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

200. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead made calculated decisions to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

201. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

202. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

203. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

204. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

205. Plaintiff and Class Members have no adequate remedy at law.

206. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury as described herein.

207. Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all

applicable regulations, industry standards, and federal, state, or local laws;

iii. Requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. Prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network

is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. Requiring Defendant to conduct regular database scanning and securing checks;

xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both

internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect herself; and

xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: June 21, 2023

Respectfully submitted,

s/ Gary M. Klinger

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Counsel for Plaintiff and the Proposed Class